FortiClient (Windows) - Release Notes

Version 6.0.4

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET COOKBOOK
https://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

December 10, 2018
FortiClient (Windows) 6.0.4 Release Notes
04-604-524552-20181210

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-12-10	Initial release of FortiClient (Windows) 6.0.4.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 6.0.4 build 0182.

Review all sections prior to installing FortiClient.

Licensing

FortiClient offers two licensing modes:

- Standalone mode
- Managed mode

Standalone mode

In standalone mode, FortiClient is not connected to a FortiGate or FortiClient Enterprise Management Server (EMS). In this mode, FortiClient is free for private individuals and commercial businesses to use. No license is required.

Support for FortiClient in standalone mode is provided on the Fortinet Forums (forum.fortinet.com). Phone support is not provided.

Managed mode

Companies with large installations of FortiClient usually need a means to manage their endpoints. EMS can be used to provision and centrally manage FortiClient endpoints, and FortiGate can be used with FortiClient endpoints for network security. Each FortiClient endpoint can connect to a FortiGate or an EMS. In this mode, FortiClient licensing is applied to the FortiGate or EMS. No separate license is required on FortiClient itself.

When using the ten (10) free licenses for FortiClient in managed mode, support is provided on the Fortinet Forums (forum.fortinet.com). Phone support is not provided when using the free licenses. Phone support is provided for paid licenses.

FortiClient licenses on the FortiGate

FortiGate 30 series and higher models include a FortiClient license for ten (10) free, connected FortiClient endpoints. For additional connected endpoints, you must purchase a FortiClient license subscription. Contact your Fortinet sales representative for information about FortiClient licenses.

FortiClient licenses on the EMS

EMS includes a FortiClient license for ten (10) free, connected FortiClient endpoints for evaluation. For additional connected endpoints, you must purchase a FortiClient license subscription. Contact your Fortinet sales representative for information about FortiClient licenses.

Special Notices

Nested VPN tunnels

Parallel, independent VPN connections to different sites are not supported; however, FortiClient VPN connection may still be established over existing third-party (for example, AT&T Client) VPN connection (nested tunnels).

Microsoft Windows server support

For Microsoft Windows servers, the AntiVirus and Vulnerability Scan features for FortiClient are supported.

Rebranding tool not supported

FortiClient (Windows) 6.0.4 does not support the FortiClient Rebranding Tool.

Installation Information

Firmware images and tools

The following files are available in the firmware image file folder:

File	Description
FortiClientSetup_6.0.xx.xxxx.exe	Standard installer for Microsoft Windows (32-bit)
FortiClientSetup_6.0.xx.xxxx.zip	A zip package containing FortiClient.msi and language transforms for Microsoft Windows (32-bit). Some properties of the MSI package can be customized with FortiClient Configurator tool
FortiClientSetup_6.0.xx.xxxx_x64.exe	Standard installer for Microsoft Windows (64-bit)
FortiClientSetup_6.0.xx.xxxx_x64.zip	A zip package containing FortiClient.msi and language transforms for Microsoft Windows (64-bit). Some properties of the MSI package can be customized with FortiClient Configurator tool
FortiClientTools_6.0.xx.xxxx.zip	A zip package containing miscellaneous tools, including VPN Automation files

The following tools and files are available in the FortiClientTools_6.0.xx.xxxx.zip file:

File	Description
FortiClientVirusCleaner	A virus cleaner
OnlineInstaller	This file downloads and installs the latest FortiClient file from the public FDS
SSLVPNcmdline	Command line SSL VPN client
SupportUtils	Includes diagnostic, uninstallation, and reinstallation tools
VPNAutomation	A VPN automation tool

Please review the following sections prior to installing FortiClient version 6.0.4: Introduction on page 5, Special Notices on page 7, and Product Integration and Support on page 10.

Installation options

When installing FortiClient version 6.0.4, you can choose the setup type that best suits your needs. FortiClient will always install the Fortinet Security Fabric Agent (SFA) feature and enable the Vulnerability Scan feature by default. You

can select to install one or more of the following options:

- Secure Remote Access: VPN components (IPsec and SSL) will be installed.
- Advanced Persistent Threat (APT) Components: FortiSandbox detection and quarantine features will be installed.
- Additional Security Features: Select one or more of the following to install them: AntiVirus, Web Filtering, Single Sign On, Application Firewall

It is recommended to not install VPN components on Windows Server systems if not required.

Upgrading from previous FortiClient versions

FortiClient version 6.0.4 supports upgrade from FortiClient versions 5.4 and later.

If you are deploying an upgrade from FortiClient 5.6.2 or earlier versions via FortiClient EMS and the upgrade fails, uninstall FortiClient on the endpoints, then deploy the latest version of FortiClient.

Downgrading to previous versions

Downgrading FortiClient version 6.0.4 to previous FortiClient versions is not supported.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal located at https://support.fortinet.com. After logging in, click on *Download* > *Firmware Image Checksums*, enter the image file name, including the extension, and select *Get Checksum Code*.

Product Integration and Support

FortiClient 6.0.4 support

The following table lists version 6.0.4 product integration and support information.

FortiClient 6.0.4 support information

Desktop Operating Systems	• Microsoft Windows 7 (32-bit and 64-bit) • Microsoft Windows 8, 8.1 (32-bit and 64-bit) • Microsoft Windows 10 (32-bit and 64-bit) FortiClient 6.0.4 does not support Microsoft Windows XP and Microsoft Windows Vista.
Server Operating Systems	• Microsoft Windows Server 2008 R2 or newer FortiClient 6.0.4 does not support Windows Server Core.
Minimum System Requirements	• Microsoft Windows compatible computer with Intel processor or equivalent • Compatible operating system and minimum 512MB RAM • 600MB free hard disk space • Native Microsoft TCP/IP communication protocol • Native Microsoft PPP dialer for dial-up connections • Ethernet network interface controller (NIC) for network connections • Wireless adapter for wireless network connections • Adobe Acrobat Reader for viewing FortiClient documentation • Windows Installer MSI installer version 3.0 or later
FortiAnalyzer	• 6.0.0 and later • 5.6.0 and later
FortiAuthenticator	• 4.3.1 • 4.3.0 • 4.2.1 FortiToken Mobile push notification is not supported for the following versions: • 4.2.0 • 4.1.0 and later • 3.3.0 and later • 3.2.0 and later • 3.1.0 and later • 3.0.0 and later
FortiClient EMS	• 6.0.0 and later
FortiManager	• 6.0.0 and later • 5.6.0 and later
FortiOS	• 6.0.0 and later

	• 5.6.0 and later Only IPsec VPN and SSL VPN are supported with the following FortiOS versions: • 5.4.0 and later
FortiSandbox	• 3.0.0 and later • 2.5.0 and later The following version is supported, but may require authorization of FortiClient to be disabled. To disable authorization run the FortiSandbox CLI command: `device-authorization -f` • 2.4.0 and later The following supported versions do not offer authorization of FortiClient: • 2.3.0 and later • 2.2.0 and later • 2.1.0

Language support

The following table lists FortiClient language support information.

Language	Graphical user interface	XML configuration	Documentation
English	Yes	Yes	Yes
Chinese (simplified)	Yes		
Chinese (traditional)	Yes		
French (France)	Yes		
German	Yes		
Japanese	Yes		
Korean	Yes		
Portuguese (Brazil)	Yes		
Russian	Yes		
Spanish (Spain)	Yes		

The FortiClient language setting defaults to the regional language setting configured on the client workstation, unless configured in the XML configuration file.

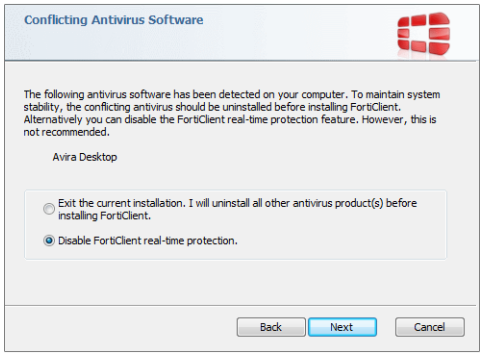
If the client workstation is configured to a regional language setting that is not supported by FortiClient, it defaults to English.

Conflicts with third party antivirus products

The antivirus feature in FortiClient is known to conflict with other similar products in the market.

- FortiClient's antivirus feature should not be used with other AV products.
- If not using FortiClient's antivirus feature, the FortiClient installation folder should be excluded from scanning for the third party AV product.

During a new installation of FortiClient, the installer will search for other registered third party software and, if any is found, warn users to uninstall them before proceeding with the installation. There is also an option to disable FortiClient Real Time Protection (RTP).



Resolved Issues

The following issues have been fixed in version 6.0.4. For inquiries about a particular bug, contact Customer Service & Support.

Malware Protection

Bug ID	Description
507588	AV custom scan still scans files in the exclusion list.
515437	FortiClient still showed Sandbox-related setting even when Sandbox was not installed.
516431	FortiClient Sandbox still shows to submit trusted files on network driver.
517974	FortiClient does not send files to FortiSandbox when client retrieve email attachment using Python.
521175	Windows Security Center on Windows 10 shows FortiClient RTP enabled even if AV is disabled on the client.
522022	Quick/full scan cause BSOD on Windows 7.
524253	Exclusion list failed to work for on-demand scan and scheduled scan.
527051	Missed application for file eqnedt.exe in FortiClient antiexploit support table.

Web Filter

Bug ID	Description
518719	Web Filter still uses the previous IP address when network/DNS changed and fdg1.fortigate.com is resolved to a new IP.
518873	New empty line was added to the host file after each enabling then disabling Safe Search configuration.
519501	Investigate and implement Safe Search via hosts file for more search engines.

Remote Access

Bug ID	Description
472223	Unable to select certificate for SSL VPN.
505191	Remote Access (IPsec) loses saved username/password when upgrading to 6.0.0.
515937	ipsec.exe crashes in VCRUNTIME140.dll, version : 14.0.24210.0.
516544	Cannot save username with certificate in SSL VPN (profile managed by EMS).
518061	Windows SSL VPN hostcheck by guid does not work (from FortiClient GUI).
526547	SSL auto-connect when off-net issue.

Vulnerability Scan

Bug ID	Description
516394	FortiClient freezes on the patching progress screen and also causes the host machine to hang up.

GUI

Bug ID	Description
483523	Black screen for a few minutes after login/logoff.
516056	FortiClient GUI failed to show VCM scan when EMS triggered VCM scan.
525536	FortiClient 6.0.3 assertion fail when clicking on Vulnerability Scan tab.

Install and upgrade

Bug ID	Description
518592	FortiClient 6.0.3 failed to upgrade to new FortiClient version from FortiTray when using RDP session.

Other

Bug ID	Description
481003	FortiClient causing longer logon time to terminal server (Citrix) for first user.
515911	FortiClient EMS console in *Software Inventory* > *Applications* section incorrectly shows Cyrillic characters.
516289	SSO Mobility - Silent install with two FortiAuthenticators.
516736	BSOD observed on x64 Windows 8.1 in ST environment.
522496	FCDBLog.exe keeps crashing.
525990	FortiClient user avatar agent crashes every time when user logs in.

Known Issues

The following issues have been identified in FortiClient (Windows) 6.0.4. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Endpoint Control

Bug ID	Description
505768	FortiClient EMS does not show VPN and Application Firewall events.
515473	Hiding any feature (except Application Firewall) will cause FortiClient (Windows) to report feature as installed and not enabled.
524864	FortiClient (Windows) sends wrong most recent Vulnerability Scan time to EMS.

Malware Protection

Bug ID	Description
496084	AV exclusion list does not work in on-demand scan if %windir% or %systemroot% variables are used.
514009	FortiClient failed to inject into Firefox application.
514547	FortiClient quick scan failed to move quarantined files to FortiClient quarantine folder.
516704	AV should recognize Windows-signed files.
519096	FortiClient failed to log USB block action for Google Pixel 2.
519098	Potential wrong block state for USB access after FortiClient was uninstalled.
524528	FortiClient always set security risk categories allowed when AV feature was disabled and block_malicious_websites =0
526845	Excluded folder is misrepresented in FortiClient GUI after importing a configuration.
526855	Writing EICAR to remote folder succeeds.
527068	FortiClient failed to quarantine eicar files in outlook attachment.

Web Filter

Bug ID	Description
519244	fortisniff2.sys crashes on FortiClient (Windows) 6.0.2
523108	Web filter exclusion list should accept URL up to 2083 characters long.

Application Firewall

Bug ID	Description
517351	Application gets blocked when Firewall is enabled.
526255	Application Firewall interrupting "Architect" application without any block.

Remote Access

Bug ID	Description
504291	FortiClient with IPv6 only configuration fails to connect with remote IKE 2 IPv6 IPsec tunnel.
513932	No CERT payload sent by FortiClient (Windows) during IKEv2 certificate authentication.
514115	FortiClient lost saved password after disconnecting IPsec VPN.
514799	Split DNS does not include news.163.com when configured for 163.com.
516244	Changing or saving VPN setting should not remove IPv6 <remote_networks><network>.
516658	Disabling automatic maintenance from EMS does not delete the schedule in Windows client task scheduler.
522348	IPsec IKEv2 VPN does not disconnect when WiFi connection is lost.
525460	On FortiClient (Windows) 6.0.3 autoconnect does not retry to connect if the connection fails the first time.
525542	After laptop boot or wake-up, FortiClient (Windows) will try to autoconnect even though it is onnet.
528434	Failed to see VPN before logon option on Win10x64 1803 with fresh install of FortiClient.

GUI

Bug ID	Description
525449	Javascript error while connecting VPN, issue on version 6.0.X was occurring due to admin roaming profile

Install and upgrade

Bug ID	Description
413419	FortiClient and EMS server should prevent installation and upgrade to unsupported OS versions.

Other

Bug ID	Description
458729	Admin cannot define multiple FortiAnalyzer for remote logging
518771	FortiShield blocks Forticlient.exe from changing registry - FA_Scheduler.
519995	FortiClient profile has certs when EMS profile does not.
524127	Event messages and context are duplicated and incorrect.
525219	Incorrect message when maximum licenses exceeded.
525869	FortiClient (Windows) does not provide any message when wrong password is provided to restore back.